# BENT FUNCTIONS GENERALIZING DILLON'S PARTIAL SPREAD FUNCTIONS

WILLIAM M. KANTOR

Abstract. This note presents generalizations of the partial spread bent functions introduced by Dillon, as well as the corresponding relative difference sets in nonabelian groups.

## 1. Introduction

In his thesis, Dillon introduced bent functions obtained using partial spreads of $\mathbb{Z}_2$-vector spaces – and, more generally, sets of subgroups of a group [6, 7]. Generalized versions of this notion have been obtained using desarguesian spreads ([9], [3, Theorem 40], [12], [15, Theorem 2.5]) and partial spreads [14]. The present note provides a generalization (Theorem 2.2) of Dillon's bent functions involving groups, using what amount to partial spreads and proved using elementary bookkeeping but no exponential sums. All of the preceding results are special cases. We conclude with another special case (Theorem 3.3) using a proof involving exponential sums.

Since bent functions produce relative difference sets [17, p. 6], we obtain large numbers of relative difference sets in groups that need not be abelian (Corollary 2.9).

## 2. Partial spreads of groups

Let $G$ and $H$ be finite groups.

**Definition 2.1.** A function $f\colon G \to H$ is *bent* if, whenever $1 \neq z \in G$, $x \mapsto f(xz)f(x)^{-1}$ takes each value in $H$ equally often (i. e., $|G|/|H|$ times).

This definition is trivially equivalent to the requirement that $\{(x, f(x)) \mid x \in G\}$ is a difference set in $G \times H$ relative to $1 \times H$ [17, p. 6]. Such a function $f$ is called "perfect nonlinear" in [16].

The following is our main result:

**Theorem 2.2.** *In a group $G$ of order $(qN)^2$, let $\Sigma$ be a set of $(q-1)N$ subgroups of order $qN$ any two of which intersect only in 1. Let $H$ be a group of order $q$. Partition $\Sigma$ into $q-1$ subsets $\Sigma_i$ of size $N$ ($i \in H\backslash\{1\}$); let $D_i := \cup\Sigma_i\backslash\{1\}$ and $D_1 := G\backslash \cup_{i\neq 1} D_i$. Then the function $f\colon G \to H$, defined by $f(D_i) = i$ for all $i \in H$, is bent.*

**Proof.** It is crucial here that (*) *$\{D_i \mid i \in H\}$ partitions $G$*. We need to show that there are exactly $qN^2$ solutions $x$ to the equation $f(xz)f(x)^{-1} = b$ whenever $1 \neq z \in G$ and $b \in H$. Thus, for each $z$ and $b$ we need to determine

$$\sum_{c,d} |(D_c z^{-1}) \cap D_d| \quad \text{where } c, d \in H \text{ satisfy } cd^{-1} = b. \tag{2.3}$$

*Key words and phrases.* bent function, partial spread, relative difference set.
This research was supported in part by a grant from the NSA.

Let $k$ be the unique element of $H$ such that $z \in D_k$. We always *assume that $i$ and $j$ denote elements of $H\backslash\{1\}$*, but $k$ may be 1. If $k \neq 1$ let $z \in \tilde{X}_k \in \Sigma_k$. (The tilde is included in order to distinguish among subgroups in the same set $\Sigma_i$ when $k = i$: if $k \neq i$ then we delete the tilde.)

We proceed in several steps.

$$|D_i| = N(qN-1), \ |D_1| = qN^2 + qN - N. \tag{2.4}$$

The first of these follows from $|\Sigma_i| = N$, and the second from (*).

$$|(D_i z^{-1}) \cap D_j| = (N - \delta_{ik})(N - \delta_{jk}) \ \text{ if } \ i \neq j. \tag{2.5}$$

For, if $X_i \in \Sigma_i, X_j \in \Sigma_j$, then the equation $z = x_j^{-1} x_i$ $(x_i \in X_i,\, x_j \in X_j)$ has a (unique) solution for distinct $i, j, k$, and no solution if $X_i = \tilde{X}_k$ or $X_j = \tilde{X}_k$.

$$|(D_i z^{-1}) \cap D_i| = (N - \delta_{ik})(N - \delta_{ik} - 1) + (qN-2)\delta_{ik}. \tag{2.6}$$

For, if $X_i, X_i' \in \Sigma_i$, then the equation $z = x_i'^{-1} x_i$ $(x_i \in X_i,\, x_i' \in X_i')$ has a unique solution precisely when $z \notin X_i, X_i'$ and $X_i \neq X_i'$; $qN-2$ solutions when $X_i = X_i' = \tilde{X}_k$ (since we must have $x_i, x_i' \neq 1$); and no solution otherwise.

$$|(D_i z^{-1}) \cap D_1| = |(D_1 z^{-1}) \cap D_i| = (N + 1 - \delta_{1k})(N - \delta_{ik}) + \delta_{ik}. \tag{2.7}$$

For, $|(D_i z^{-1}) \cap D_1| = |D_i z^{-1}| - \sum_{j \neq i} |(D_i z^{-1}) \cap D_j| - |(D_i z^{-1}) \cap D_i|$ by (*). Now use (2.4)-(2.6) and an elementary calculation.

$$|(D_1 z^{-1}) \cap D_1| = (N + 1 - \delta_{1k})(N - \delta_{1k}) + \delta_{1k} qN. \tag{2.8}$$

For, $|(D_1 z^{-1}) \cap D_1| = |D_1| - \sum_i |(D_i z^{-1}) \cap D_1|$ by (*). Now use (2.4) and (2.7).

Two equally elementary calculations using (2.4)-(2.8) and $\sum_c \delta_{ck} = 1$ show that (2.3) equals $qN^2$ for all $b \in H$ (considering the cases $b \neq 1$ and $b = 1$ separately). $\square$

**Remark 1. Group structure.** Unfortunately, if $G$ is not elementary abelian, when $q = 2$ there are very few examples of groups having sets $\Sigma$ meeting our requirements [8], and when $q > 2$ there are no examples [10, Theorems 3.3, 3.4]. Therefore, the preceding theorem only deals with elementary abelian groups $G$ when $q > 2$.

On the other hand, it seems unexpected that *the definition of $f$ does not require any special properties of the group $H$*, so that nonisomorphic groups $H$ of order $q$ produce bent functions $f\colon G \to H$ using the same partition of $\Sigma$.

**Remark 2. How many relative difference sets?** It is not uncommon to provide constructions of combinatorial objects and assume that many inequivalent objects arise if there are many choices made in the construction [6, 7, 3, 9, 12, 14, 15]. Proving that there are, indeed, many inequivalent objects is another matter, one that can be difficult.

We already noted that bent functions correspond to relative difference sets. Relative difference sets in nonisomorphic groups $G \times H$ are clearly inequivalent. There are certainly many examples showing that the structure of $H$ is usually involved in such a relative difference set, unlike in the theorem.

If $|H| = p^s$ with $p$ prime, then the number of nonisomorphic groups $H$ is large: $p^{(2/27)s^3 + O(s^{8/3})}$ [2]. The number of inequivalent possibilities for the set $\Sigma$ is far larger [11]. However, cruder estimates than in [11] already give information in groups that need not be abeian (see [17, p. 6] for the parameters of a relative difference set):

**Corollary 2.9.** *For integers $m \geq s \geq 1$ and a prime $p$, let $G$ be an elementary abelian $p$-group of order $p^{2m}$ and let $H$ be any group of order $p^s$. Then there are more than $p^{p^{m-1}-9m^2}$ pairwise inequivalent $(p^{2m}, p^s, p^{2m}, p^{2m-s})$-difference sets in $G \times H$ relative to $1 \times H$.*

**Proof.** "Inequivalence" means "in different $\mathrm{Aut}(G \times H)$-orbits". Clearly $|\mathrm{Aut}(G \times H)| < p^{(2m+s)^2} \leq p^{(3m)^2}$. The number of possible sets $\Sigma$ inside a desarguesian spread of $G$ is $\binom{p^m+1}{p^{m-1}} \geq p^{p^{m-1}}$, producing more than $p^{p^{m-1}-9m^2}$ inequivalent relative difference sets. $\square$

Note that the above estimate did not even take into account the many ways to partition a given choice $\Sigma$. Far more bent functions and relative difference sets are obtained from the Maiorana-McFarland bent functions (cf. [7], [13, p. 51] and [3, Theorem 39]) using similar simple estimates, but those only use elementary abelian groups $G \times H$.

**Remark 3. Association schemes.** In the notation of the theorem, the sets $D_i$ produce an association scheme, obtained by partitioning $G \times G$ into the sets $\{(x, x) \mid x \in G\}$ and $\{(x, y) \in G \times G \mid 1 \neq xy^{-1} \in D_i\}$, $i \in H$ (compare [4, esp. p. 114]).

## 3. Vector spaces

We now turn to a different type of proof of a special case of Theorem 2.2, and another brief discussion of the number of different bent functions obtained.

Let $V$ be a finite vector space over a field $K$ of characteristic $p$. There are two equivalent definitions of bent functions $V \to K$ [1, Theorem 2], [15, Theorem 2.3]. The first is a special case of Definition 2.1:

**Definition 3.1.** (Combinatorial definition.) $f: V \to K$ is *bent* if, whenever $0 \neq z \in V$, $v \mapsto f(v+z) - f(v)$ takes each value in $K$ equally often (i.e., $|V|/|K|$ times).

Let $\zeta$ denote a primitive complex $p$th root of 1. Fix a nonzero linear functional $T: K \to \mathbb{Z}_p$, as well as a basis and hence a dot product for the $K$-space $V$. For $f: V \to K$ and $k \in K$, write $f_k(v) := \zeta^{T(kf(v))}$ and

$$\hat{f}(u) := \sum_{v \in V} \zeta^{T(u \cdot v + f(v))}, \ u \in V.$$

**Definition 3.2.** (Fourier definition.) $f: V \to K$ is *bent* if $|\hat{f}_k(u)| = |V|^{1/2}$ for all $k \in K^*, u \in V$. (This notion is independent of the choice of dot product and $T$.)

A function is *balanced* if each member of the codomain occurs as a value equally often (compare Definitions 2.1 and 3.1. This amounts to a labelled partition of the domain into sets of equal size, where the number of parts is the size of the codomain.

A finite *prequasifield* $(F, +, *)$ of characteristic $p$ consists of a finite vector space $F$ over $\mathbb{Z}_p$, together with a binary operation $*$ on $F$ such that $a*(x+y) = a*x+a*y$ and $z \mapsto a*z - b*z$ is bijective for all $x, y, a, b \in F$, $a \neq b$. The associated *spread* consists of the following $|F|+1$ subspaces of $F \oplus F$: $x = 0$, and all $y = m * x$ for $m \in F$; note the similarity to the situation in Theorem 2.2. The associated *kernel* is the field consisting of all additive maps $k: F \to F$ such that $m * (kx) = k(m * x)$ for all $m, x \in F$. Both the prequasifield and the spread determine a finite affine

plane [5, p. 220] that will not be needed here; nor will the fact that the same spread can arise from many non-isomorphic prequasifields.

We use Definition 3.2 in order to provide an entirely different type of proof of the following special case of Theorem 2.2:

**Theorem 3.3.** *Let $(F,+,*)$ be a prequasifield of characteristic $p$ whose kernel contains the field $K$. Fix a $K$-basis of $F$ and hence of $V := F\oplus F$, and equip $F$ and $V$ with the corresponding dot products. Let $g\colon F\to K$ be any balanced function. Then $f\colon V\to K$ is a bent function, where $f(0,y) := g(0)$, and $f(x,y) := g(m)$ with $y = m*x$ for a unique $m\in F$ when $x\neq 0$.*

**Proof.** (Compare [3, Theorem 40].) Clearly, $\hat f_k(a,b) = \sum_{x,y}\zeta^{T((a,b)\cdot(x,y)+kf(x,y))}$. If $m\in F$ let $L_m\colon F\to F$ be the $K$-linear map defined by $L_m(x) = m*x$; and let $L_m^t$ be its transpose, so that $b\cdot L_m(x) = L_m^t(b)\cdot x$ for all $b,x\in F$. If $x\in F^*$ and $y\in F$ then below we will write $(x,y) = (x,m*x)$ for a unique $m\in F$. For each $k\in K^*$ and $(a,b)\in V$,

$$\begin{aligned}
\hat f_k(a,b) &= \sum_{x\in F^*,m\in F}\zeta^{T((a,b)\cdot(x,m*x)+kf(x,m*x))} + \sum_{y\in F}\zeta^{T(b\cdot y+kf(0,y))}\\
&= \sum_{x\in F^*,m\in F}\zeta^{T(a\cdot x+b\cdot(m*x))}\zeta^{T(kg(m))} + \sum_{y\in F}\zeta^{T(b\cdot y+kg(0))}\\
&= \sum_{m\in F}\zeta^{T(kg(m))}\sum_{x\in F^*}\zeta^{T(a\cdot x+b\cdot L_m(x))} + \sum_{y\in F}\zeta^{T(b\cdot y+kg(0))}\\
&= \sum_{m\in F}\zeta^{T(kg(m))}\sum_{x\in F}\zeta^{T([a+L_m^t(b)]\cdot x)} - \sum_{m\in F}\zeta^{T(kg(m))} + \sum_{y\in F}\zeta^{T(b\cdot y+kg(0))}\\
&= \sum_{m\in F}\zeta^{T(kg(m))}\sum_{x\in F}\zeta^{T([a+L_m^t(b)]\cdot x)} + \sum_{y\in F}\zeta^{T(b\cdot y+kg(0))};
\end{aligned}$$

here $\sum_m\zeta^{T(kg(m))} = 0$ since $\sum_0^{p-1}\zeta^j = 0$ and $m\mapsto T(kg(m))$ is balanced.

The transformations $L_m, m\in F$, have the property that the difference of any two is nonsingular; hence the same is true of their transposes $L_m^t, m\in F$, so that $m\mapsto L_m^t(b)$ is 1-1 and hence onto if $b\neq 0$. Given $b\neq 0$ and $a$ it follows that there is a unique $\tilde m\in F$ such that $a+L_{\tilde m}^t(b) = 0$. For that $\tilde m$ and each $m'\neq\tilde m$, we have $\sum_{x\in F}\zeta^{T([a+L_{m'}^t(b)]\cdot x)} = 0$ since $x\mapsto T([a+L_{m'}^t(b)]\cdot x)$ is balanced. Since $y\mapsto T(b\cdot y+kg(0))$ is also balanced, $\hat f_k(a,b) = \zeta^{T(kg(\tilde m))}\sum_{x\in F}\zeta^0+0 = \zeta^{T(kg(\tilde m))}|F|$ has absolute value $|F|$.

Finally, when $b=0$ we find that $\hat f_k(a,0) = \sum_{m\in F}\zeta^{T(kg(m))}\sum_{x\in F}\zeta^{T(a\cdot x)} + \sum_{y\in F}\zeta^{T(kg(0))} = 0\sum_{x\in F}\zeta^{T(a\cdot x)} + \zeta^{T(kg(0))}|F|$ has absolute value $|F|$. □

**Remark 4.** By [11], using subsets $\Sigma$ of a desarguesian spread in Theorem 3.3 (so the quasifield is just a field) produces at least $\binom{q^m+1}{q^{m-1}}\Big/2(q^m+1)q^m(q^m-1)^2\log_p q^m$ pairwise affinely-inequivalent bent functions on $V$ (compare Remark 2). Although there are many many different types of nondesarguesian spreads known, there are not enough known to change the preceding estimate significantly.

## References

[1] A. C. Ambrosimov, Properties of the bent functions of $q$-ary logic over finite fields. Discrete Math. Appl. 4, 341–350 (1994).

[2] S. R. Blackburn, P. M. Neumann and G. Venkataraman. Enumeration of finite groups. Cambridge Tracts in Math. 173, Cambridge U. Press, 2007.

[3] C. Carlet and C. Ding, Highly nonlinear mappings. J. Complexity 20, 205–244 (2004).

[4] E. R. van Dam and M. Muzychuk, Some implications on amorphic association schemes. J. Comb. Theory (A) 117, 111–127 (2010).

[5] P. Dembowski, Finite geometries. Springer, Berlin–Heidelberg–NY 1968.

[6] J. F. Dillon, Elementary Hadamard difference sets. Ph.D. thesis, U. of Maryland 1974.

[7] J. F. Dillon, Elementary Hadamard difference sets, pp. 237–249 in: Proc. Sixth Southeastern Conf. Combinatorics, Graph Theory, and Computing. Winnipeg 1975.

[8] D. Frohardt, Groups with a large number of large disjoint subgroups. J. Algebra 107, 153–159 (1987).

[9] X. D. Hou, $q$-ary bent functions constructed from chain rings. Finite Fields Appl. 4, 55–61 (1998).

[10] D. Jungnickel, Existence results for translation nets, II. J. Algebra 122 288–298 (1989).

[11] W. M. Kantor, Exponential numbers of two-weight codes, difference sets and symmetric designs. Discrete Math. 46, 95–98 (1983).

[12] S. Kim, G.-M. Gil, K.-H. Kim and J.-S. No, Generalized bent functions constructed from partial spreads, p. 41 in: IEEE Intl. Symp. Information Theory, IEEE, Piscataway NJ, 2002.

[13] P. V. Kumar, R. A. Scholtz and L. R. Welch, Generalized bent functions and their properties. J. Comb. Theory (A) 40, 90–107 (1985).

[14] P. Lisonek and H. Y. Lu (submitted).

[15] K. Nyberg, Perfect nonlinear S-boxes, pp. 378–386 in: EUROCRYPT'91, Proc. 10th Intl. Conf. Theory and Application of Cryptographic Techniques. Lecture Notes in Computer Science 547, Springer, Berlin-Heidelberg 1991.

[16] L. Poinsot, Non abelian bent functions. Cryptogr. Commun. 4, 1–23 (2012).

[17] B. Schmidt, Characters and cyclotomic fields in finite geometry. Springer, Berlin 2002.

College of Computer and Information Science, Northeastern U., Boston, MA 02115
*E-mail address*: kantor@uoregon.edu